



National Security Agency/Central Support Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Risk Monitoring Capability

Version 1.1.1

Risk Monitoring assesses the effectiveness of the risk decisions that are made by the Enterprise. This Capability establishes the current security posture and then determines the gaps between the current security posture and the intended risk posture (see the Risk Analysis Capability). Risk Monitoring includes the monitoring of risks (as identified in the Risk Identification Capability) pertaining to people, operations, technology, and environments. Risk levels must be monitored based on changes in the risk posture.



# CGS Risk Monitoring Capability

Version 1.1.1



## Table of Contents

1	Revisions .....	2
2	Capability Definition .....	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions .....	5
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations .....	6
7	Capability Interrelationships.....	7
7.1	Required Interrelationships .....	7
7.2	Core Interrelationships .....	10
7.3	Supporting Interrelationships.....	10
8	Security Controls .....	11
9	Directives, Policies, and Standards .....	12
10	Cost Considerations .....	17
11	Guidance Statements .....	17



# CGS Risk Monitoring Capability

Version 1.1.1



## 1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1



# CGS Risk Monitoring Capability

Version 1.1.1



## 2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Risk Monitoring assesses the effectiveness of the risk decisions that are made by the Enterprise. This Capability establishes the current security posture and then determines the gaps between the current security posture and the intended risk posture (see the Risk Analysis Capability). Risk Monitoring includes the monitoring of risks (as identified in the Risk Identification Capability) pertaining to people, operations, technology, and environments. Risk levels must be monitored based on changes in the risk posture.

## 3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Risk Monitoring examines the decisions made and the mitigations applied to reduce risk in an Enterprise and assesses the effectiveness of those decisions. It identifies the gap between the intended level of risk (risk posture) and the actual level of risk (security posture). Risk Monitoring observes all Enterprise risks, including people, operations, technology, and environments and also examines the business value of risk decisions. Risk Monitoring shall continually consider the Enterprise’s changing risk posture as provided by the Risk Analysis Capability.

Risk Monitoring is highly dependent on the other Capabilities that manage risk in the Enterprise (i.e., Risk Identification, Risk Analysis, and Risk Mitigation). Risk Identification enumerates the risks. Risk Analysis makes decisions about the risks and establishes the accepted risk posture. Risk Mitigation implements the necessary measures to bring risks to an acceptable level. As risks and factors contributing to risks change, they are identified and analyzed by Risk Identification and Risk Analysis, respectively.

The Risk Monitoring Capability shall use a Plan of Actions and Milestones (POA&M) for programs to document actions taken to apply the mitigations or other implementation



# CGS Risk Monitoring Capability

Version 1.1.1



information. The maintenance of the POA&M shall be the responsibility of the Program Managers or Program Management Office (PMO). The Risk Monitoring Capability shall employ services from a Program Manager or PMO to ensure that all activities and resources are managed according to the program management (PM) plan and are able to track and implement the mitigations assigned.

Risk Monitoring provides information about whether the countermeasures implemented by Risk Mitigations are effective. Risk Monitoring determines the Enterprise security posture using information provided by Risk Mitigation and the Detect Events Capabilities. The security posture is the actual state of risk in the Enterprise at a given point in time. The security posture is compared against the risk posture. The risk posture is the intentionally assumed position of what the state of Enterprise risk shall be, as determined by Risk Identification and Risk Analysis. The difference between the security posture (actual state of risk) and the risk posture (intended state of risk) is what the Risk Monitoring Capability measures to determine the effectiveness of the Risk Mitigations.

The Risk Monitoring Capability calculates numerical values as a means of quantifying the risk posture and security posture. The difference between these two values is known as the risk gap result. The use of numerical quantifiers is standardized by the Enterprise or Community for the quantifiers' values to be useful across the Enterprise and its boundaries. Risk gap results are assessed in the context of the Enterprise and the mission. Smaller risk gap result values are better because that means that Risk Mitigations are more effective.

The Risk Monitoring Capability shall operate at a frequency that is determined by the mission needs and the changing Enterprise environment and risks. This frequency could be periodic or near real-time. Risk Monitoring frequency is limited by the rate of the information that flows into it from the other Manage Risk Capabilities.

Risk Monitoring results shall be aggregated and centrally managed at the Enterprise level. Raw data produced by Risk Monitoring shall be managed at the local enclave level or at the Enterprise level, depending on the size of the Enterprise. Based on the monitoring needs, access to raw data shall be provided to Enterprise stakeholders and managers. The aggregation of results may be performed at each level of the management hierarchy within the Enterprise. The benefit of performing aggregation in this manner is that managers at each level of the hierarchy can be informed about the areas for which they are responsible.



# CGS Risk Monitoring Capability

Version 1.1.1



All Risk Monitoring information (reports and raw data) shall be communicated via an out-of-band network. Information about a network's risks and weaknesses shall never be stored on that network for security reasons. This information shall be treated at the same or higher level of classification as the data it refers to. Systems that contain monitoring data employ Data Protection, System Protection, Communication Protection, and Contingency Planning mechanisms. Archiving of the aggregated results or raw data is policy and mission driven. Personnel who perform technical Risk Monitoring functions shall be dedicated personnel with the authority to take action based on the Risk Monitoring reporting, in accordance with Enterprise policy.

Risk Monitoring shall provide reports to all relevant stakeholders, as determined by mission needs. These stakeholders can include management, information technology (IT), and information assurance (IA) personnel. Risk Monitoring reports are useful for management personnel because they provide a business context for resources allocated to Risk Mitigation purposes. IT and IA personnel use Risk Monitoring reports to help identify implementation weaknesses. Specific reporting requirements are determined by mission needs. Reports shall follow a Community standardized format so they can be easily shared with other Enterprises, when necessary. Report content may be tailored to suit the needs of the recipient based on the risk decision being made.

## 4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Risk will change over time.
2. Acceptable levels of risk will change over time.
3. Activities and missions will change over time and with it, their associated level of risk.
4. A risk management process has been established.
5. Capabilities have been implemented that provide data to determine the security posture.
6. All programs have an established PM role or office to manage activities and resources.





# CGS Risk Monitoring Capability

Version 1.1.1



## 5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability monitors risk decision results for all Enterprise assets (including people, operations, technology, and environment).
2. The Capability takes into consideration that acceptable levels of risk change.
3. Mission context is considered during evaluation of the security posture.

## 6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

The Organization will use the Risk Monitoring Capability to evaluate the effectiveness of its Risk Mitigation measures and its risk decisions. To effectively implement Risk Monitoring, the Organization will determine the current security posture (as indicated by Risk Mitigation and the Detect Events Capabilities). This will be compared with the risk posture (as defined by the Risk Identification and Risk Analysis Capabilities). Both the risk posture and security posture will be established in the context of the mission and the Organization. The Organization will calculate the risk and security postures as numerical values for analysis purposes. Determining the difference in value between the risk posture and the security posture is how the Organization will assess the effectiveness of Risk Mitigation. That gap between where the Organization wants to be (risk posture) and where it is (security posture) with regard to risk is what tells the Organization how effective Risk Mitigation is at reducing risk. The smaller the gap is, the more effective the Risk Mitigation measures are.

The Organization will use metrics to determine values for the risk and security postures. Processes and tools used for Risk Monitoring will enable federated use of results in the environment and will be in compliance with any applicable Community-established policies or standards. The Organization will employ dedicated personnel to perform Risk Monitoring tasks.



# CGS Risk Monitoring Capability

Version 1.1.1



The Organization will operate its Risk Monitoring functions at a frequency that is set by mission needs, and the rate of change to the Enterprise environment and risk levels. Because Risk Monitoring is so highly dependent on the output of the other Manage Risk Capabilities, those Capabilities will be adjusted when necessary so they can provide output at the appropriate pace.

The Organization will define the hierarchy of responsibility for Risk Monitoring and reporting. Different Risk Monitoring functions require different data. Functions performed at the lowest level require the collection and analysis of raw data. This data will be summarized, in the form of reports, and provided to the next level for decision-making and awareness. As necessary, the reporting will be abstracted to meet the needs of the report consumer. Risk Monitoring report consumers include managerial and technical personnel, who analyze the reports based on how they enable or inhibit mission flow. The reason for this hierarchy is centralized information aggregation. Each level typically will need only the output from the next level down but will have access to raw data when necessary.

The Organization will format its Risk Monitoring reports according to any applicable Community standards to allow for easy information sharing, where appropriate. Specific requirements for reports will be derived from mission need. Regular reports will be generated for applicable Organization personnel to ensure that they are kept up to date about the current status of the Enterprise risk and Risk Mitigation effectiveness.

## 7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

### 7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping—The Risk Monitoring Capability relies on the Network Mapping Capability to provide information that is used as an input for its analysis to determine the Enterprise security posture.
- Network Boundary and Interfaces—The Risk Monitoring Capability relies on the Network Boundary and Interfaces Capability to provide information that is used as an input for its analysis to determine the Enterprise security posture.





# CGS Risk Monitoring Capability

Version 1.1.1



- Utilization and Performance Management–The Risk Monitoring Capability relies on the Utilization and Performance Management Capability to provide information that is used as an input for its analysis to determine the Enterprise security posture.
- Understand Mission Flows–The Risk Monitoring Capability relies on the Understand Mission Flows Capability to provide information that is used as an input for its analysis to determine the Enterprise security posture.
- Understand Data Flows–The Risk Monitoring Capability relies on the Understand Data Flows Capability to provide information that is used as an input for its analysis to determine the Enterprise security posture.
- Hardware Device Inventory–The Risk Monitoring Capability relies on the Hardware Device Inventory Capability to provide information that is used as an input for its analysis to determine the Enterprise security posture.
- Software Inventory–The Risk Monitoring Capability relies on the Software Inventory Capability to provide information that is used as an input for its analysis to determine the Enterprise security posture.
- Understand the Physical Environment–The Risk Monitoring Capability relies on the Understand the Physical Environment Capability to provide information that is used as an input for its analysis to determine the Enterprise security posture.
- System Protection–The Risk Monitoring Capability relies on the System Protection Capability to provide information that is used to evaluate the effectiveness of protections to determine the Enterprise security posture. The Risk Monitoring Capability also relies on the System Protection Capability to protect risk data.
- Communication Protection–The Risk Monitoring Capability relies on the Communication Protection Capability to provide information that is used to evaluate the effectiveness of protections to determine the Enterprise security posture. The Risk Monitoring Capability also relies on the Communication Protection Capability to protect risk data while in transit.
- Physical and Environmental Protections–The Risk Monitoring Capability relies on the Physical and Environmental Protections Capability to provide information that is used to evaluate the effectiveness of protections to determine the Enterprise security posture.
- Personnel Security–The Risk Monitoring Capability relies on the Personnel Security Capability to provide information that is used to evaluate the effectiveness of protections to determine the Enterprise security posture.
- Network Access Control–The Risk Monitoring Capability relies on the Network Access Control Capability to provide information that is used to evaluate the effectiveness of protections to determine the Enterprise security posture.



# CGS Risk Monitoring Capability

Version 1.1.1



- Configuration Management—The Risk Monitoring Capability relies on the Configuration Management Capability to provide information that is used to evaluate the effectiveness of protections to determine the Enterprise security posture.
- Port Security—The Risk Monitoring Capability relies on the Port Security Capability to provide information that is used to evaluate the effectiveness of protections to determine the Enterprise security posture.
- Network Boundary Protection—The Risk Monitoring Capability relies on the Network Boundary Protection Capability to provide information that is used to evaluate the effectiveness of protections to determine the Enterprise security posture.
- Identity Management—The Risk Monitoring Capability relies on the Identity Management Capability to provide information that is used to determine the Enterprise security posture.
- Access Management—The Risk Monitoring Capability relies on the Access Management Capability to provide information that is used to determine the Enterprise security posture.
- Key Management—The Risk Monitoring Capability relies on the Key Management Capability to provide information that is used to determine the Enterprise security posture.
- Digital Policy Management—The Risk Monitoring Capability relies on the Digital Policy Management Capability to provide information that is used to determine the Enterprise security posture.
- Metadata Management—The Risk Monitoring Capability relies on the Metadata Management Capability to provide information that is used to determine the Enterprise security posture.
- Credential Management—The Risk Monitoring Capability relies on the Credential Management Capability to provide information that is used to determine the Enterprise security posture.
- Attribute Management—The Risk Monitoring Capability relies on the Attribute Management Capability to provide information that is used to determine the Enterprise security posture.
- Data Protection—The Risk Monitoring Capability relies on the Data Protection Capability to provide information that is used to determine the Enterprise security posture. The Risk Monitoring Capability also relies on the Data Protection Capability to protect risk data.



# CGS Risk Monitoring Capability

Version 1.1.1



- Network Enterprise Monitoring—The Risk Monitoring Capability relies on the Network Enterprise Monitoring Capability for information, which is used to determine the Enterprise security posture.
- Physical Enterprise Monitoring—The Risk Monitoring Capability relies on the Physical Enterprise Monitoring Capability for information, which is used to determine the Enterprise security posture.
- Personnel Enterprise Monitoring—The Risk Monitoring Capability relies on the Personnel Enterprise Monitoring Capability for information, which is used to determine the Enterprise security posture.
- Network Intrusion Detection—The Risk Monitoring Capability relies on the Network Intrusion Detection Capability for information, which is used to determine the Enterprise security posture.
- Host Intrusion Detection—The Risk Monitoring Capability relies on the Host Intrusion Detection Capability for information, which is used to determine the Enterprise security posture.
- Network Hunting—The Risk Monitoring Capability relies on the Network Hunting Capability for information, which is used to determine the Enterprise security posture.
- Physical Hunting—The Risk Monitoring Capability relies on the Physical Hunting Capability for information, which is used to determine the Enterprise security posture.
- Enterprise Audit Management—The Risk Monitoring Capability relies on the Enterprise Audit Management Capability for information, which is used to determine the Enterprise security posture.
- Risk Identification—The Risk Monitoring Capability relies on the Risk Identification Capability to provide information about threat and vulnerability pairs.
- Risk Analysis—The Risk Monitoring Capability relies on the Risk Analysis Capability to provide information about the mission impact of risks.
- Risk Mitigation—The Risk Monitoring Capability relies on information from the Risk Mitigation Capability about mitigations that have been implemented.

## 7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management—The Risk Monitoring Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards—The Risk Monitoring Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about



# CGS Risk Monitoring Capability

Version 1.1.1



applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.

- IA Awareness—The Risk Monitoring Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Risk Monitoring Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities—The Organizations and Authorities Capability establishes the roles and responsibilities assigned to the Risk Monitoring Capability. For instance, the PM role is established and governed under the Organizations and Authorities Capability. The Risk Monitoring Capability measures the effectiveness of roles and responsibilities defined by Organizations and Authorities.

## 7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Incident Response—The Risk Monitoring Capability relies on the Incident Response for information that provides situational awareness.
- Incident Analysis—The Risk Monitoring Capability relies on the Incident Analysis for information that provides situational awareness.

## 8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	
CA-2 SECURITY ASSESSMENTS	Control: The organization: b. Assesses the security controls in the information system [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to



# CGS Risk Monitoring Capability

Version 1.1.1



	<p>meeting the security requirements for the system;</p> <p>c. Produces a security assessment report that documents the results of the assessment; and</p> <p>d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.</p> <p>Enhancement/s:</p> <p>(1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.</p> <p>(2) The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security testing]].</p>
CA-7 CONTINUOUS MONITORING	<p>Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:</p> <p>b. A determination of the security impact of changes to the information system and environment of operation;</p> <p>c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and</p> <p>d. Reporting the security state of the information system to appropriate organizational officials [Assignment: organization-defined frequency].</p> <p>Enhancement/s:</p> <p>(1) The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.</p> <p>(2) The organization plans, schedules, and conducts assessments [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security assessment]] to ensure compliance with all vulnerability mitigation procedures.</p>
PM-4 PLAN OF	<p>Control: The organization implements a process for ensuring that</p>





# CGS Risk Monitoring Capability

Version 1.1.1



<b>ACTION AND MILESTONES PROCESS</b>	plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Enhancement/s: None Specified.
<b>RA-3 RISK ASSESSMENT</b>	Control: The organization: d. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. Enhancement/s: None Specified

## 9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

### Risk Monitoring Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 503, IC Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008, Unclassified	Summary: This directive establishes Intelligence Community (IC) policy for information technology (IT) systems security risk management and certification and accreditation (C&A). It directs the use of standards for IT risk management established, published, issued, and promulgated by the IC Chief Information Officer (CIO), which may include standards, policies, and guidelines approved by the National Institute of Standards and Technology (NIST) and/or the Committee on National Security Systems (CNSS). Risk Monitoring is an important element of the risk management process.
ICD 801, Acquisition, 16 August 2009, Unclassified	Summary: National Intelligence Program (NIP) major system acquisitions (MSA) shall be undertaken using a balanced and proactive risk management approach to create innovative and responsive systems for use by the IC.





# CGS Risk Monitoring Capability

Version 1.1.1



	Proactive risk management is the acceptance of appropriate risk to allow the necessary innovation and technology insertion in an acquisition, while ensuring, through positive means, that the uncertainties of the acquisition are managed within a tolerable range to enable cost, schedule, and performance constraints to be met. Risk Monitoring is an important element of a proactive risk management approach.
ODNI/CIO-2008-108, Committee on National Security Systems (CNSS) Agreement to Use National Institutes of Standards and Technology (NIST) Documents as Basis for Information Security Controls and Risk Management, 20 April 2009, Unclassified	Summary: Documented CNSS intent for federal agencies, IC, and the Department of Defense (DoD), to use the same set of standards, controls, and procedures to secure government information systems; and committee consensus to assist NIST in incorporating National Security Systems (NSS) requirements within NIST policies and instructions that define information security controls to protect systems and information (NIST Special Publication [SP] 800-53 v3), as well as the NIST instructions for assessing systems (SP 800-37) and performing risk management (SP 800-30 and SP 800-39). Risk Monitoring is an important phase in performing risk management.
<b>Comprehensive National Cybersecurity Initiative (CNCI)</b>	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
<b>Department of Defense (DoD)</b>	
DoDD O-8530.1, Computer Network Defense (CND), 8 January 2001, Classified	Summary: This directive establishes Computer Network Defense (CND) policy, definition, and responsibilities for CND within the DoD, including the implementation of robust infrastructure and information assurance (IA) practices, such as regular and proactive vulnerability analysis and assessment, including active penetration testing and Red Teaming, and implementation of identified improvements; and adherence to a defense-in-depth strategy using risk



# CGS Risk Monitoring Capability

Version 1.1.1



	management principles to defend against both external and internal threats .... Risk Monitoring is an important element of the risk management process.
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: This instruction provides joint policy and guidance for IA and CND operations. Policy includes a. The risk management process will consider the Mission Assurance Category (MAC) of the system, the classification or sensitivity of information handled (i.e., processed, stored, displayed, or transmitted) by the system, potential threats, documented vulnerabilities, protection measures, and need-to-know.... c. Risk management will be conducted and integrated in the life cycle for information systems. There must be a specific schedule for periodically assessing and mitigating mission risks caused by major changes to the IT system and processing environment due to changes resulting from policies and new technologies. Risk Monitoring is an important element in conducting risk management.
Risk Management Guide for DoD Acquisition, version 2.0, June 2003, Unclassified	Summary: This document provides acquisition professionals and program management offices with a practical reference for dealing with system acquisition risks; it discusses risk and risk management, examines risk management concepts relative to the DoD acquisition process, discusses the implementation of a risk management program from the program management office perspective, and describes a number of techniques that address the aspects (phases) of risk management, i.e., planning, assessment, handling, and monitoring.
Committee for National Security Systems (CNSS)	
CNSSP-22, Information Assurance Risk Management Policy for National Security Systems, February 2009, Unclassified	Summary: This document establishes the requirements for Enterprise IA risk management within the national security community, which requires a holistic view of the IA risks to NSS, operating within the Enterprise using disciplined processes, methods, and tools. It provides a framework for decision-makers to continuously evaluate and prioritize IA risks in order to accept or recommend strategies to remediate or mitigate those risks to an acceptable level. Risk



# CGS Risk Monitoring Capability

Version 1.1.1



	Monitoring is an important element of the risk management framework (RMF).
Other Federal (OMB, NIST, ...)	
OMB M-10-15, Memorandum for Heads of Executive Departments and Agencies, 21 April 2010, Unclassified	Summary: Agencies need to have an Enterprise-wide system to continuously monitor security-related information in a way that is both manageable and actionable. Agency stakeholders need to have relevant security information delivered in a timely manner. Agencies must develop automated risk models for monitoring threats and vulnerabilities.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

## Risk Monitoring Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP 800-30, Risk Management Guide for	Summary: This SP provides a foundation for the development of an effective risk management program,



# CGS Risk Monitoring Capability

Version 1.1.1



Information Technology Systems, July 2002, Unclassified	containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. Risk Monitoring is an important element of an effective risk management program.
NIST SP 800-37 Rev-1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010, Unclassified	This publication transforms the traditional C&A process into the six-step RMF. It provides guidelines for applying the RMF to federal information systems including conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011, Unclassified	Summary: This SP provides guidelines for managing risk to organizational operations, organizational assets, individuals, other Organizations, and the nation resulting from the operation and use of information systems. It implements an RMF, a structured, yet flexible approach for managing that portion of risk resulting from the incorporation of information systems into the mission and business processes of an Organization. Risk Monitoring is an important element of an RMF.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Nothing found	

## 10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)



# CGS Risk Monitoring Capability

Version 1.1.1



2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Solution used for implementation—The use of an automated versus manual or partially automated solution will affect the direct cost and operating costs.
2. Manpower to implement, maintain, and execute—A manual solution will require personnel to need significantly more man hours to operate.

## 11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Risk Monitoring Capability.

- The Enterprise shall conduct risk monitoring to examine the risk decisions made and the mitigations applied to reduce risk in an Enterprise and assess the effectiveness of those decisions.
- Risk monitoring activities shall observe all Enterprise risks, including people, operations, environments, and the business value of risk decisions.
- Risk monitoring activities shall continually consider the Enterprise's changing risk posture.
- Risk monitoring activities shall employ the use of a POA&M for programs to document actions taken to apply the mitigations or other implementation information.
- The applicable Program Manager or PMO shall be responsible for the maintenance of a POA&M.



# CGS Risk Monitoring Capability

Version 1.1.1



- The Enterprise shall employ services from a Program Manager or PMO to ensure that all activities and resources are managed according to the PM plan and are able to track and implement the mitigations assigned.
- Risk monitoring activities shall provide information to the Enterprise about whether the risk mitigation countermeasures that have been implemented are effective.
- Risk monitoring activities shall determine the security posture (actual state of risk at a given point in time) for the Enterprise.
- The Enterprise shall measure the difference between the security posture (actual state of risk) and the risk posture (intended state of risk) to determine the effectiveness of risk mitigation countermeasures.
- The Enterprise shall calculate numerical values as a means of quantifying the risk posture and security posture, and subsequent risk gap, which is the difference between these two values.
- The use of numerical quantifiers shall be standardized by the Enterprise or Community to enable sharing across Enterprise boundaries.
- Risk gap results shall be assessed in the context of the Enterprise and mission.
- Risk monitoring activities shall operate at a frequency that is determined by the mission needs and the changing Enterprise environment and risks. This frequency could be periodic or near real-time.
- Risk monitoring results shall be aggregated and centrally managed at the Enterprise level.
- Raw data produced by risk monitoring activities shall be managed at the local enclave or Enterprise level, depending on the size of the Enterprise.
- Access to raw risk monitoring data shall be provided to Enterprise stakeholders and managers, as necessary.
- All risk monitoring information (reports and raw data) shall be communicated via an out-of-band network.
- All risk monitoring information (reports and raw data) shall be protected at the same or higher level of classification as the data it refers to.
- Risk monitoring information (reports and raw data) shall be archived in accordance with Enterprise policy and mission needs.
- Personnel engaged in risk monitoring activities shall be dedicated personnel with the authority to take action based on risk monitoring reporting, in accordance with Enterprise policy.
- The Enterprise shall provide risk monitoring reports to all relevant stakeholders, as determined by mission needs.





# CGS Risk Monitoring Capability

Version 1.1.1



- Specific reporting requirements for risk monitoring shall be determined by mission needs and may be tailored to suit the needs of the recipient based on the risk decision being made.
- Risk monitoring reports shall follow a Community standardized format.